Durham University

Durham Research Online

Deposited in DRO:

07 October 2020

Version of attached file:

Accepted Version

Peer-review status of attached file:

Peer-reviewed

Citation for published item:

Kazda, Alexandr and Opršal, Jakub and Valeriote, Matt and Zhuk, Dmitriy (2020) 'Deciding the existence of minority terms.', Canadian mathematical bulletin., 63 (3). pp. 577-591.

Further information on publisher's website:

https://doi.org/10.4153/S0008439519000651

Publisher's copyright statement:

This article has been published in a revised form in Canadian mathematical bulletin http://doi.org/10.4153/S0008439519000651. This version is published under a Creative Commons CC-BY-NC-ND. No commercial re-distribution or re-use allowed. Derivative works cannot be distributed. © Canadian Mathematical Society 2019.

Additional information:

Use policy

The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in DRO
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Please consult the full DRO policy for further details.

Durham University Library, Stockton Road, Durham DH1 3LY, United Kingdom
Tel : +44 (0)191 334 3042 | Fax : +44 (0)191 334 2971
https://dro.dur.ac.uk

arXiv:1901.00316v2 [math.LO] 8 Oct 2019

DECIDING THE EXISTENCE OF MINORITY TERMS

ALEXANDR KAZDA, JAKUB OPRŠAL, MATT VALERIOTE,
AND DMITRIY ZHUK

Abstract. This paper investigates the computational complexity of deciding if a given finite idempotent algebra has a ternary term operation m that satisfies the minority equations $m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx y$. We show that a common polynomial-time approach to testing for this type of condition will not work in this case and that this decision problem lies in the class NP.

1. Introduction

It is not difficult to see that for the 2-element group $\mathbb{Z}_2 = \langle \{0,1\}, + \rangle$, the term operation $m(x,y,z) = x + y + z$ satisfies the equations

$$m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx y. \tag{1}$$

A slightly more challenging exercise is to show that a finite Abelian group will have such a term operation if and only if it is isomorphic to a Cartesian power of $\mathbb{Z}_2$.

A ternary operation $m(x,y,z)$ on a set A is called a *minority operation on* A if it satisfies the identities (1). A ternary term $t(x,y,z)$ of an algebra $\mathbf{A}$ is a *minority term of* $\mathbf{A}$ if its interpretation as an operation on A, $t^{\mathbf{A}}(x,y,z)$, is a minority operation on A. Given a finite algebra $\mathbf{A}$, one can decide if it has a minority term by constructing all of its ternary term operations and checking to see if any of them satisfy the equations (1). Since the set of ternary term operations of $\mathbf{A}$ can be as big as $|A|^{|A|^3}$, this procedure will have a runtime that in the worst case will be exponential in the size of $\mathbf{A}$.

In this paper we consider the computational complexity of testing for the existence of a minority term for finite algebras that are idempotent. An n-ary operation f on a set A is *idempotent* if it satisfies the equation $f(x,x,\dots,x) \approx x$ and an algebra is *idempotent* if all of its basic operations are. We observe that every minority operation is idempotent. While idempotent algebras are rather special, one can always form one by taking the *idempotent reduct* of a given algebra $\mathbf{A}$. This is the algebra with universe A whose basic operations are all of the idempotent term operations of $\mathbf{A}$. It

2010 *Mathematics Subject Classification.* Primary 68Q25, Secondary 03B05, 08A40.

The first author was supported by the Charles University grants PRIMUS/SCI/12 and UNCE/SCI/22. The second author was supported by European Research Council (Grant Agreement no. 681988, CSP-Infinity) and UK EPSRC (Grant EP/R034516/1), and the third author was supported by the Natural Sciences and Engineering Council of Canada.

turns out that many important properties of an algebra and the variety that it generates are governed by its idempotent reduct [9].

The condition of an algebra having a minority term is an example of a more general existential condition on the set of term operations of an algebra called a *strong Maltsev condition*. Such a condition consists of a finite set of operation symbols along with a finite set of equations involving them. An algebra is said to satisfy the condition if for each k-ary operation symbol from the condition, there is a corresponding k-ary term operation of the algebra so that under this correspondence, the equations of the condition hold. For a more careful and complete presentation of this notion and related ones, we refer the reader to [6].

Given a strong Maltsev condition Σ, the problem of determining if a finite algebra satisfies Σ is decidable and lies in the complexity class EXPTIME. As in the minority term case, one can construct all term operations of an algebra up to the largest arity of an operation symbol in Σ and then check to see if any of them can be used to witness the satisfaction of the equations of Σ. In general, we cannot do any better than this, since for some strong Maltsev conditions, it is known that the corresponding decision problem is EXPTIME-complete [5].

The situation for finite idempotent algebras appears to be better than in the general case since there are a number of strong Maltsev conditions for which there are polynomial-time procedures to decide if a finite idempotent algebra satisfies them [5, 7, 8]. At present there is no known characterization of these strong Maltsev conditions and we hope that the results of this paper may help to lead to a better understanding of them. We refer the reader to [3] or to [1] for background on the basic algebraic notions and results used in this work.

2. Formulation of the problem

In this section, we formally introduce the considered problem. In all the problems mentioned in the introduction, we assume that the input algebra is given as a list of tables of its basic operations. In particular, this implies that the input algebra has finitely many operations. We also assume that the input algebra has at least one operation (i.e., the input is non-empty) and we forbid nullary operations on the input. The main concern of this paper is the following decision problem.

Definition 1. Define $\mathsf{Minority}^{\mathrm{Id}}$ to be the following decision problem:

- INPUT: A list of tables of basic operations of an idempotent algebra $\mathbf{A}$.
- QUESTION: Does $\mathbf{A}$ have a minority term?

The size of an input is measured by the following formula. For a finite algebra $\mathbf{A}$, let

$$\|\mathbf{A}\| = \sum_{i=1}^{\infty} k_i |A|^i,$$

where k_i is the number of i-ary basic operations of $\mathbf{A}$. Since we assume that $\mathbf{A}$ has only finitely many operations, the sum is finite. Also note that $\|\mathbf{A}\| \geq |A|$ since we assumed that $\mathbf{A}$ has a non-nullary operation.

3. Minority is a join of two weaker conditions

One approach to understanding the minority term condition is to see if maybe there exist two weaker Maltsev conditions Σ_1 and Σ_2 such that a finite algebra $\mathbf{A}$ has a minority term if and only if $\mathbf{A}$ satisfies both Σ_1 and Σ_2. In this situation, we would say that the minority term condition is the join of Σ_1 and Σ_2. Were this the case, we could decide if $\mathbf{A}$ has a minority term by deciding Σ_1 and Σ_2.

On the surface, the minority term condition is already quite concise and natural; it is not clear if having a minority term can be expressed as a join of weaker conditions. In this section, we show that it is a join of having a Maltsev term with a condition which we call having a minority-majority term (not to be confused with the 'generalized minority-majority' terms from [4]). Maltsev terms are a classical object of study in universal algebra – deciding if an algebra has them is in P for finite idempotent algebras. The minority-majority terms are much less understood.

Definition 2. A ternary term $p(x, y, z)$ of an algebra $\mathbf{A}$ is a *Maltsev term for* $\mathbf{A}$ if it satisfies the equations

$$p(x, x, y) \approx p(y, x, x) \approx y$$

and a 6-ary term $t(x_1, \ldots, x_6)$ is a *minority-majority term* of $\mathbf{A}$ if it satisfies the equations

$$\begin{aligned} t(y, x, x, z, y, y) &\approx y \\ t(x, y, x, y, z, y) &\approx y \\ t(x, x, y, y, y, z) &\approx y. \end{aligned}$$

We point out that if an algebra has a minority term then it also, trivially, has a Maltsev term, but that the converse does not hold (as witnessed by the cyclic group $\mathbb{Z}_4$). Our definition of a minority-majority term is a strengthening of the term condition found by Olšák in [12]. Olšák has shown that his terms are a weakest non-trivial strong Maltsev condition whose terms are all idempotent.

We observe that by padding variables, any algebra that has a minority term or a majority term (just replace the final occurrence of the variable y in the equations (1) by the variable x to define such a term) also has a minority-majority term. Since the 2-element lattice has a majority term

but no minority term, it follows that having a minority-majority term is strictly weaker than having a minority term.

Theorem 3. *An algebra has a minority term if and only if it has a Maltsev term and a minority-majority term.*

Proof. The discussion preceding this theorem establishes one direction of this theorem. For the other we need to show that if an algebra $\mathbf{A}$ has a Maltsev term $p(x, y, z)$, and a minority-majority term $t(x_1, \dots, x_6)$ then $\mathbf{A}$ has a minority term. Given such an algebra $\mathbf{A}$, define

$$m(x, y, z) = t(x, y, z, p(z, x, y), p(x, y, z), p(y, z, x)).$$

Verifying that $m(x, y, z)$ is a minority term for $\mathbf{A}$ is straightforward; we show one of the three required equalities here as an example:

$$\begin{aligned} m(x, x, y) &\approx t(x, x, y, p(y, x, x), p(x, x, y), p(x, y, x)) \\ &\approx t(x, x, y, y, y, p(x, y, x)) \approx y. \end{aligned}$$

□

Corollary 4. *The problem of deciding if a finite algebra has a minority term can be reduced to the problems of deciding if it has a Maltsev term and if it has a minority-majority term.*

As was demonstrated in [5, 7], there is a polynomial-time algorithm to decide if a finite idempotent algebra has a Maltsev term. Therefore, should testing for a minority-majority term for finite idempotent algebras prove to be tractable, then this would lead to a fast algorithm for testing for a minority term, at least for finite idempotent algebras. From the hardness results found in [5] it follows that in general, the problem of deciding if a finite algebra has a minority-majority term is EXPTIME-complete; the complexity of this problem restricted to idempotent algebras is unknown.

4. Local Maltsev terms

In [5, 7, 8, 13] polynomial-time algorithms are presented for deciding if certain Maltsev conditions hold in the variety generated by a given finite idempotent algebra. One particular Maltsev condition that is addressed by all of these papers is that of having a Maltsev term. In all but [5], the polynomial-time algorithm produced is based on testing for the presence of enough 'local' Maltsev terms in the given algebra.

Definition 5. Let $\mathbf{A}$ be an algebra and $S \subseteq A^2 \times \{0, 1\}$. A term operation $t(x, y, z)$ of $\mathbf{A}$ is a *local Maltsev term operation for* S if:

- whenever $((a, b), 0) \in S$, $t(a, b, b) = a$, and
- whenever $((a, b), 1) \in S$, $t(a, a, b) = b$.

Clearly, if $\mathbf{A}$ has a Maltsev term then it has a local Maltsev term operation for every subset S of $A^2 \times \{0, 1\}$ and conversely, if $\mathbf{A}$ has a local Maltsev term operation for $S = A^2 \times \{0, 1\}$ then it has a Maltsev term. In [7, 8, 13] it is

shown that if a finite idempotent algebra $\mathbf{A}$ has local Maltsev term operations for all two element subsets of $A^2 \times \{0,1\}$ then $\mathbf{A}$ will have a Maltsev term. This fact is then used as the basis for a polynomial-time test to decide if a given finite idempotent algebra has a Maltsev term.

In this section we extract an additional piece of information from this approach to testing for a Maltsev term, namely that if a finite idempotent algebra has a Maltsev term, then we can produce an operation table or a circuit for a Maltsev term operation in time polynomial in the size of the algebra. We will first prove that there is an algorithm for producing circuits for a Maltsev function; the algorithm for producing the operation table will then be given as a corollary. However, for the reduction presented in Section 6 we need only the algorithm for producing a function table.

Let us first briefly describe how to get a global Maltsev operation from local ones. Assume we know (circuits of) a local Maltsev term operation $t_{a,b,c,d}(x,y,z)$ for each two element subset

$$\{((a,b),0),((c,d),1)\}$$

of $A^2 \times \{0,1\}$. These are required for $\mathbf{A}$ to have a Maltsev term. A global Maltsev term can be constructed from them in two stages: First, we construct, for each $a, b \in A$, an operation $t_{a,b}$ such that $t_{a,b}(a,b,b) = a$ and $t_{a,b}(x,x,y) = y$ for all $x, y \in A$. This is done by fixing an enumeration (a_1,b_1), (a_2,b_2), $\ldots$, (a_{n^2},b_{n^2}) of A^2, and then defining, for $1 \leq j \leq n^2$, the operation $t^j_{a,b}(x,y,z)$ on A inductively as follows:

- $t^1_{a,b}(x,y,z) = t_{a,b,a_1,b_1}(x,y,z)$, and
- for $1 \leq j < n^2$, $t^{j+1}_{a,b}(x,y,z) = t_{a,b,u,v}(t^j_{a,b}(x,y,z), t^j_{a,b}(y,y,z), z)$, where $u = t^j_{a,b}(a_{j+1}, a_{j+1}, b_{j+1})$ and $v = b_{j+1}$.

An easy inductive argument shows that $t^j_{a,b}(a,b,b) = a$ and $t^j_{a,b}(a_i,a_i,b_i) = b_i$ for all $i \leq j \leq n^2$, and so setting $t_{a,b}(x,y,z) = t^{n^2}_{a,b}(x,y,z)$ works.

In the second stage, we construct a term $t_j(x,y,z)$ such that $t_j(a,a,b) = b$ for all a, $b \in A$ and $t_j(a_i,b_i,b_i) = a_i$ for all $i \leq j$. We define this sequence of operations inductively again:

- $t_1(x,y,z) = t_{a_1,b_1}(x,y,z)$, and
- for $1 \leq j < n^2$, $t_{j+1}(x,y,z) = t_{u,v}(x, t_j(x,y,y), t_j(x,y,z))$, where $u = a_{j+1}$ and $v = t_j(a_{j+1}, b_{j+1}, b_{j+1})$.

Again, it can be shown that for $1 \leq j \leq n^2$, the operation $t_j(x,y,z)$ satisfies the claimed properties and so $t_{n^2}(x,y,z)$ will be a Maltsev term operation for $\mathbf{A}$.

From the above construction, one can obtain a term that represents a Maltsev term operation of the algebra $\mathbf{A}$, starting with terms representing the operations $t_{a,b,c,d}$. But there is an efficiency problem with this approach: the term is extended by one layer in each step, which results in a term of exponential size. Therefore, the bookkeeping of this term would increase the running time of the algorithm beyond polynomial. Nevertheless, this

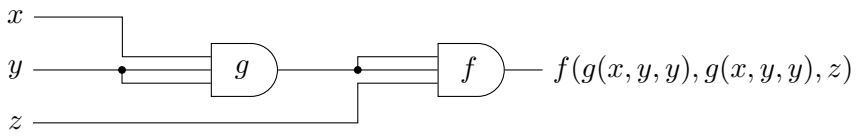

FIGURE 1. A succinct circuit representation of the term $f(g(x, y, y), g(x, y, y), z)$.

can be circumvented by constructing a succint representation of the term operations, namely by considering circuits instead of terms.

Informally, a circuit over an algebraic language (as a generalization of logical circuits) is a collection of gates labeled by operation symbols, where the number of inputs of each gate corresponds to the arity of the operation symbol. The inputs are either connected to outputs of some other gate, or designated as inputs of the circuit; an output of one of the gates is designated as an output of the circuit. Furthermore, these connections allow for straightforward evaluation, i.e., there are no oriented cycles.

Formally, we define an n-ary *circuit* in the language of an algebra $\mathbf{A}$ as a directed acyclic graph with possibly multiple edges that has two kinds of vertices: *inputs* and *gates*. There are exactly n inputs, labeled by variables $x_1, \dots, x_n$, and each of them is a source, and a finite number of gates. Each gate is labeled by an operation symbol of $\mathbf{A}$, the in-degree corresponds to the arity of the operation, and the in-edges are ordered. One of the vertices is designated as the *output* of the circuit. We define the size of the circuit to be the number of its vertices.

The value of a circuit given an input tuple $a_1, \dots, a_n$ is defined by the following recursive computation: The value on an input vertex labeled by x_i is a_i, the value on a gate labeled by g is the value of the operation $g^{\mathbf{A}}$ applied to the values of its in-neighbours in the specified order. Finally, the output value of the circuit is the value of the output vertex. It is easy to see that the value of a circuit on a given tuple can be computed in linear time (in the size of the circuit) in a straightforward way. For a fixed circuit the function that maps the input tuple to the output is a term function of $\mathbf{A}$. Indeed, to find such a term it is enough to evaluate the circuit in the free (term) algebra on the tuple $x_1, \dots, x_n$. The converse is also true since any term can be represented as a 'tree' circuit (it is an oriented tree if we omit all input vertices). Many terms can be expressed by considerably smaller circuits. We give one such example in Figure 1.

In the proof of the theorem below, we will also use circuits with multiple outputs. The only difference in the definition is that several vertices are designated as outputs. Any such circuit then computes a tuple of term functions.

Theorem 6. *Let $\mathbf{A}$ be a finite idempotent algebra. There is an algorithm whose runtime can be bounded by a polynomial in the size of $\mathbf{A}$ that will*

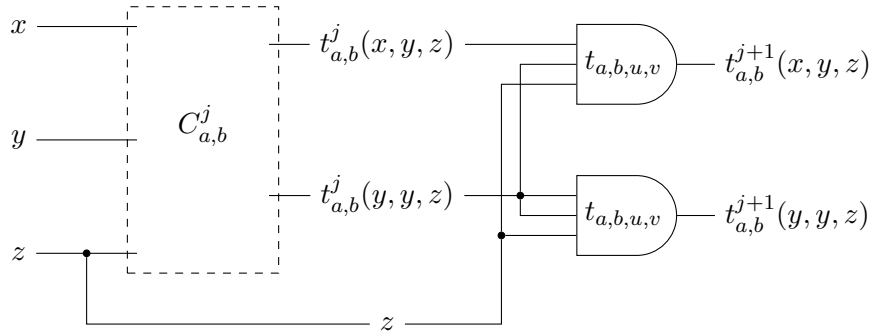

FIGURE 2. Recursive definition of circuit $C^{j+1}_{a,b}$.

either (correctly) output that $\mathbf{A}$ *has no Maltsev term operation, or output a circuit for some Maltsev term operation of* $\mathbf{A}$.

Proof. Let $n = |A|$. Recall that $\mathbf{A}$ has at least one basic operation of positive arity and hence $\|\mathbf{A}\| \geq n$. Let $m \geq 1$ be the maximal arity of an operation of $\mathbf{A}$.

We construct a circuit representing a Maltsev operation in three steps: The first step produces, for each a, b, c, d from A, a circuit that computes a local Maltsev term operation $t_{a,b,c,d}$ as defined near the beginning of this section, the second step produces circuits that compute $t_{a,b}$, and the final step produces a circuit for a Maltsev operation t. We note that the algorithm can fail only in the first step.

Step 1: Circuits for $t_{a,b,c,d}$. For each a, b, c, d, we aim to produce a circuit that computes a local Maltsev term operation $t_{a,b,c,d}$. To do this, we consider the subuniverse R of $\mathbf{A}^2$ generated by $\{(a,c),(b,c),(b,d)\}$. According to Proposition 6.1 from [5] R can be generated in time $O(||\mathbf{A}||^2 m)$. It is clear that $\mathbf{A}$ has a local Maltsev term operation $t_{a,b,c,d}$ if and only if $(a,d) \in R$. Our algorithm produces a circuit for $t_{a,b,c,d}$ by generating elements of R one at a time and keeping track of circuits that witness the membership of these elements.

More precisely, we employ a subuniverse generating algorithm to produce a sequence $r_1 = (a,c), r_2 = (b,c), r_3 = (b,d), r_4, \ldots$ of elements of R (in time $O(||\mathbf{A}||^2 m)$) such that each r_{k+1}, for $k \geq 3$, is obtained from $r_1, \ldots, r_k$ by a single application of an operation f of $\mathbf{A}^2$. Our algorithm will also produce a sequence of ternary circuits $C^3_{a,b,c,d} \subseteq C^4_{a,b,c,d} \subseteq \ldots$ such that each $C^k_{a,b,c,d}$ has k outputs, and the values of $C^k_{a,b,c,d}$ on r_1, r_2, r_3 give $r_1, \ldots, r_k$. We define $C^3_{a,b,c,d}$ to be the circuit with no gates, and outputs x_1, x_2, x_3. The circuit $C^{k+1}_{a,b,c,d}$ is defined inductively from $C^k_{a,b,c,d}$: Consider an operation f and $r_{i_1}, \ldots, r_{i_p}$ with $i_j \leq k$ such that $r_{k+1} = f(r_{i_1}, \ldots, r_{i_p})$; add a gate labeled f to $C^k_{a,b,c,d}$ connecting its inputs with the outputs of $C^k_{a,b,c,d}$ numbered by

i_j for $j = 1, \dots, p$. We designate the output of this gate as the $(k+1)$-st output of $C^{k+1}_{a,b,c,d}$.

It is straightforward to check that the circuits $C^k_{a,b,c,d}$ satisfy the requirements. We also note that the size of $C^k_{a,b,c,d}$ is exactly k. We stop this inductive construction at some step k if $r_k = (a, d)$, in which case we produce the circuit $C_{a,b,c,d}$ from $C^k_{a,b,c,d}$ by indicating a single output to be the k-th output of $C^k_{a,b,c,d}$. If, on the other hand, we have generated all of R without producing (a, d) at any step then the algorithm halts and outputs that $\mathbf{A}$ does not have a Maltsev term operation. The soundness of our algorithm follows from the fact that $\mathbf{A}$ has a local Maltsev term $t_{a,b,c,d}$ if and only if $(a, d) \in R$ and that $\mathbf{A}$ has a Maltsev term if and only if it has local Maltsev terms $t_{a,b,c,d}$ for all a, b, c, $d \in A$. The algorithm produces circuits of size $O(n^2)$ and spends most of its time generating new elements of R; generating each $C_{a,b,c,d}$ takes time $O(\|\mathbf{A}\|^2 m)$, making the total time complexity of Step 1 to be $O(\|\mathbf{A}\|^2 mn^4)$.

Step 2: Circuits for $t_{a,b}$. At this point we assume that the functions $t_{a,b,c,d}$ are part of the signature. It is clear that the full circuit can be obtained by substituting the circuits $C_{a,b,c,d}$ for gates labeled by $t_{a,b,c,d}$, and this can be still done in polynomial time.

Our task is to obtain a circuit for $t_{a,b}$. We do this by inductively constructing circuits $C^j_{a,b}$ that compute two values of the terms $t^j_{a,b}$, namely $t^j_{a,b}(x, y, z)$ and $t^j_{a,b}(y, y, z)$. Starting with $j = 0$ and $t^0(x, y, z) = x$, we define $C^0_{a,b}$ to be the circuit with no gates and outputs x, y. Further, we define circuit $C^{j+1}_{a,b}$ inductively from $C^j_{a,b}$ by adding two gates labeled by $t_{a,b,u,v}$, where $u = t^j_{a,b}(a_{j+1}, a_{j+1}, b_{j+1})$ and $v = b_{j+1}$: the first gate has as inputs the two outputs of $C^j_{a,b}$ and z, the second gate has as inputs two copies of the second output of $C^j_{a,b}$ and z. See Figure 2 for a graphical representation. Again, it is straightforward to check that these circuits have the required properties. Also note that the size of $C^j_{a,b}$ is bounded by $2j + 3$ which is a polynomial. The final circuit $C_{a,b}$ computing $t_{a,b}$ is obtained from $C^{n^2}_{a,b}$ by designating the first output of $C^{n^2}_{a,b}$ to be the only output of $C_{a,b}$. Once we have $t_{a,b,c,d}$ in the signature, this process will run in time $O(n^2)$.

Step 3: Circuit for a Maltsev term. Again, we assume that $t_{a,b}$ are basic operations, and construct circuits C_j computing two values $t_j(x, y, y)$ and $t_j(x, y, z)$ of t_j inductively. The proof is analogous to Step 2, with the only difference that we use Figure 3 for the inductive definition. Again the time complexity is $O(n^2)$.

Each step runs in time polynomial in $\|\mathbf{A}\|$ (the time complexity is dominated by Step 1) and outputs a polynomial size circuit. This also implies that expanding the gates according to their definitions in Steps 2 and 3 can be

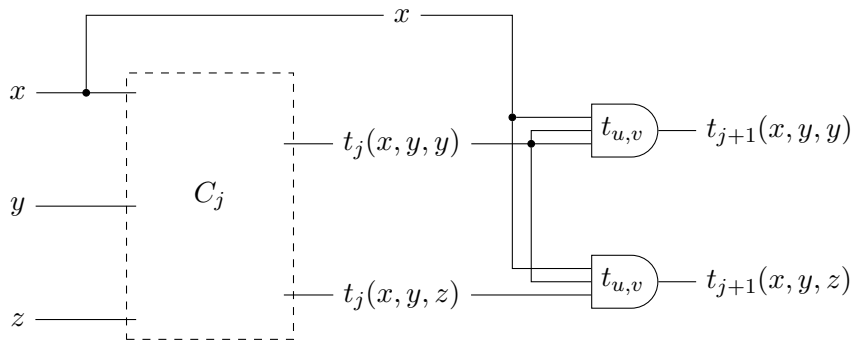

FIGURE 3. Recursive definition of circuit C_{j+1}.

done in polynomial time; the final size of the output circuit will be bounded by $O(n^6)$. □

Corollary 7. *Let* $\mathbf{A}$ *be a finite idempotent algebra. There is an algorithm whose runtime can be bounded by a polynomial in the size of* $\mathbf{A}$ *that will produce the table of some Maltsev term operation of* $\mathbf{A}$*, should one exist.*

Proof. The polynomial-time algorithm is as follows. First, generate a polynomial size circuit for some Maltsev term operation of $\mathbf{A}$. This can be done in polynomial time by the above theorem. Second, evaluate this circuit at all $|A|^3$ possible inputs. The second step runs in polynomial time since evaluation of a circuit is linear in the size of the circuit. □

We note that there is also a more straightforward algorithm for producing the operation table of a Maltsev term which follows the circuit construction but instead of circuits, it remembers the tables for each of the relevant term operations.

5. Local minority terms

In contrast to the situation for Maltsev terms highlighted in the previous section, we will show that having plenty of 'local' minority terms does not guarantee that a finite idempotent algebra will have a minority term. One consequence of this is that an approach along the lines in [7, 8, 13] to finding an efficient algorithm to decide if a finite idempotent algebra has a minority term will not work.

In this section, we will construct for each odd natural number $n > 2$ a finite idempotent algebra $\mathbf{A}_n$ with the following properties: The universe of $\mathbf{A}_n$ has size $4n$ and $\mathbf{A}_n$ does not have a minority term, but for every subset E of A_n of size $n-1$ there is a term of $\mathbf{A}_n$ that acts as a minority term on the elements of E.

We start our construction by fixing some odd $n > 2$ and some minority operation m on the set $[n] = \{1, 2, \ldots, n\}$. To make things concrete we set

$$m(x, y, z) = \begin{cases} x & y = z \\ y & x = z \\ z & \text{else,} \end{cases}$$

but note that any minority operation on $[n]$ will do.

Since there are two nonisomorphic groups of order 4, we have two different natural group operations on $\{0, 1, 2, 3\}$: addition modulo 4, which we will denote by '$+$' (its inverse is '$-$'), and bitwise XOR, which we denote by '$\oplus$' (this operation takes bitwise XOR of the binary representations of input numbers, so for example $1 \oplus 3 = 2$). Throughout this section, we will use arithmetic modulo 4, e.g., $6x = x + x$, for all expressions except those involving indices.

The construction relies on similarities and subtle differences of the two group structures, and the derived Maltsev operations, $x - y + z$ and $x \oplus y \oplus z$. Both these operations share a congruence $\equiv_2$ that is given by taking the remainder modulo 2. We note that $x \equiv_2 y$ if and only if $2x = 2y$.

Observation 8. *Let $x, y, z \in \{0, 1, 2, 3\}$. Then*

$$(x \oplus y \oplus z) - (x - y + z) \in \{0, 2\},$$

and moreover the result depends only on the classes of x, y, and z in the congruence $\equiv_2$ (i.e., the least significant binary bits of x, y, and z).

Proof. Both Maltsev operations agree modulo $\equiv_2$, hence the difference lies in the $\equiv_2$-class of 0.

To see the second part, it is enough to observe that $x \oplus 2 = x + 2 = x - 2$ for all x. Hence changing, say x to $x' = x \oplus 2$ simply flips the most significant binary bit of both $x \oplus y \oplus z$ and $x - y + z$, keeping the difference the same. □

Definition 9. Let $A_n = [n] \times [4]$. For $i \in [n]$, we define $t_i(x, y, z)$ to be the following operation on A_n:

$$t_i((a_1, b_1), (a_2, b_2), (a_3, b_3)) = \begin{cases} (i, b_1 - b_2 + b_3) & \text{if } a_1 = a_2 = a_3 = i, \text{ and} \\ (m(a_1, a_2, a_3), b_1 \oplus b_2 \oplus b_3), & \text{otherwise.} \end{cases}$$

The algebra $\mathbf{A}_n$ is defined to be the algebra with universe A_n and basic operations $t_1, \ldots, t_n$.

By construction, the following is true.

Claim 10. *For every $(n-1)$-element subset E of A_n, there is a term operation of $\mathbf{A}_n$ that satisfies the minority term equations when restricted to elements from E.*

Proof. Pick $i \in [n]$ such that no element of E has its first coordinate equal to i; the operation t_i is a local minority for this E. □

Proposition 11. *For $n > 1$ and odd, the algebra $\mathbf{A}_n$ does not have a minority term.*

Proof. Given some $(i, a) \in A_n$, we will refer to a as the *arithmetic part* of (i, a). This is to avoid talking about 'second coordinates' in the confusing situation when (i, a) itself is a part of a tuple of elements of A_n.

To prove the proposition, we will define a certain subuniverse R of $(\mathbf{A}_n)^{3n}$ and then show that R is not closed under any minority operation on A_n (applied coordinate-wise). We will write $3n$-tuples of elements of A_n as $3n \times 2$ matrices where the arithmetic parts of the elements make up the second column.

Let $R \subseteq (A_n)^{3n}$ be the set of all $3n$-tuples of the form

$$\begin{pmatrix} 1 & x_1 \\ 2 & x_2 \\ \vdots & \\ n & x_n \\ 1 & x_{n+1} \\ 2 & x_{n+2} \\ \vdots & \\ n & x_{2n} \\ 1 & x_{2n+1} \\ 2 & x_{2n+2} \\ \vdots & \\ n & x_{3n} \end{pmatrix}$$

such that

$$x_{kn+1} \equiv_2 x_{kn+2} \equiv_2 \cdots \equiv_2 x_{kn+n}, \qquad \text{for } k = 0, 1, 2, \text{ and} \tag{2}$$

$$\sum_{i=1}^{3n} x_i = 2. \tag{3}$$

The three equations from (2) mean that the least significant bits of the arithmetic parts of the first n entries agree and similarly for the second and the last n entries; equation (3) can be viewed as a combined parity check on all involved bits.

Claim 12. *The relation R is a subuniverse of $(\mathbf{A}_n)^{3n}$.*

Proof. By the symmetry of the t_i's and R, it is enough to show that t_1 preserves R. Let us take three arbitrary members of R:

$$\begin{pmatrix} 1 & x_{1,1} \\ 2 & x_{1,2} \\ \vdots & \\ n & x_{1,n} \\ 1 & x_{1,n+1} \\ 2 & x_{1,n+2} \\ \vdots & \\ n & x_{1,2n} \\ 1 & x_{1,2n+1} \\ 2 & x_{1,2n+2} \\ \vdots & \\ n & x_{1,3n} \end{pmatrix}, \begin{pmatrix} 1 & x_{2,1} \\ 2 & x_{2,2} \\ \vdots & \\ n & x_{2,n} \\ 1 & x_{2,n+1} \\ 2 & x_{2,n+2} \\ \vdots & \\ n & x_{2,2n} \\ 1 & x_{2,2n+1} \\ 2 & x_{2,2n+2} \\ \vdots & \\ n & x_{2,3n} \end{pmatrix}, \begin{pmatrix} 1 & x_{3,1} \\ 2 & x_{3,2} \\ \vdots & \\ n & x_{3,n} \\ 1 & x_{3,n+1} \\ 2 & x_{3,n+2} \\ \vdots & \\ n & x_{3,2n} \\ 1 & x_{3,2n+1} \\ 2 & x_{3,2n+2} \\ \vdots & \\ n & x_{3,3n} \end{pmatrix}$$

and apply t_1 to them to get:

$$\vec{r} = \begin{pmatrix} 1 & x_{1,1} - x_{2,1} + x_{3,1} \\ 2 & x_{1,2} \oplus x_{2,2} \oplus x_{3,2} \\ & \vdots \\ n & x_{1,n} \oplus x_{2,n} \oplus x_{3,n} \\ 1 & x_{1,n+1} - x_{2,n+1} + x_{3,n+1} \\ 2 & x_{1,n+2} \oplus x_{2,n+2} \oplus x_{3,n+2} \\ & \vdots \\ n & x_{1,2n} \oplus x_{2,2n} \oplus x_{3,2n} \\ 1 & x_{1,2n+1} - x_{2,2n+1} + x_{3,2n+1} \\ 2 & x_{1,2n+2} \oplus x_{2,2n+2} \oplus x_{3,2n+2} \\ & \vdots \\ n & x_{1,3n} \oplus x_{2,3n} \oplus x_{3,3n} \end{pmatrix} \tag{4}$$

We want to verify that $\vec{r} \in R$. First note that (2) is satisfied: This follows from the fact that $x - y + z$ and $x \oplus y \oplus z$ give the same result modulo 2, and the assumption that the original three tuples satisfied (2).

What remains is to verify the property (3). If in the equality (4) above we replace the operations $\oplus$ by $-$ and $+$, verifying (3) is easy: The sum of the arithmetic parts of such a modified tuple is

$$\sum_{j=1}^{3n}(x_{1,j} - x_{2,j} + x_{3,j}) = \sum_{j=1}^{3n} x_{1,j} - \sum_{j=1}^{3n} x_{2,j} + \sum_{j=1}^{3n} x_{3,j} = 2 - 2 + 2 = 2. \tag{5}$$

This is why we need to examine the difference between the $\oplus$-based and $+$-based Maltsev operations. For $k \in \{0, 1, 2\}$ and $i \in \{1, \dots, n\}$ we let

$$c_{k,i} = (x_{1,kn+i} \oplus x_{2,kn+i} \oplus x_{3,kn+i}) - (x_{1,kn+i} - x_{2,kn+i} + x_{3,kn+i})$$

By the second part of Observation 8, $c_{k,i}$ does not depend on i (changing i does not change the $x_{j,kn+i}$'s modulo $\equiv_2$ by condition (2) in the definition of R). Hence we can write just c_k instead of $c_{k,i}$.

Using c_0, c_1, and c_2 to adjust for the differences between the two Maltsev operations, we can express the sum of the arithmetic parts of the tuple $\vec{r}$ as

$$\sum_{j=1}^{3n}(x_{1,j} - x_{2,j} + x_{3,j}) + \sum_{i=2}^{n} c_0 + \sum_{i=2}^{n} c_1 + \sum_{i=2}^{n} c_2 = 2 + (n-1)(c_0 + c_1 + c_2)$$

where we used (5) to get the right hand side. We chose n odd, hence $n-1$ is even and each c_k is even by Observation 8, so $(n-1)c_k = 0$ for any $k = 0, 1, 2$. We see that the sum of the arithmetic parts of $\vec{r}$ is equal to 2 which concludes the proof of (3) for the tuple $\vec{r}$ and we are done. □

It is easy to see that

$$\begin{pmatrix} 1 & 0 \\ 2 & 0 \\ \vdots & \\ n & 0 \\ 1 & 1 \\ 2 & 1 \\ \vdots & \\ n & 1 \\ 1 & 1 \\ 2 & 1 \\ \vdots & \\ n & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 1 \\ \vdots & \\ n & 1 \\ 1 & 0 \\ 2 & 0 \\ \vdots & \\ n & 0 \\ 1 & 1 \\ 2 & 1 \\ \vdots & \\ n & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 1 \\ \vdots & \\ n & 1 \\ 1 & 1 \\ 2 & 1 \\ \vdots & \\ n & 1 \\ 1 & 0 \\ 2 & 0 \\ \vdots & \\ n & 0 \end{pmatrix} \in R, \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 2 & 0 \\ \vdots & \\ n & 0 \\ 1 & 0 \\ 2 & 0 \\ \vdots & \\ n & 0 \\ 1 & 0 \\ 2 & 0 \\ \vdots & \\ n & 0 \end{pmatrix} \notin R.$$

However, the last tuple can be obtained from the first three by applying any minority operation on the set A_n coordinate-wise. From this we conclude that $\mathbf{A}_n$ does not have a minority term. □

We note that the above construction of $\mathbf{A}_n$ makes sense for n even as well and claim that these algebras also have the same key features, namely, by construction, they have plenty of 'local' minority term operations but they do not have minority terms. The verification of this last fact for n even is similar, but slightly more technical than for n odd, and we omit the proof here.

The algebras $\mathbf{A}_n$ can also be used to witness that having a lot of local minority-majority terms does not guarantee the presence of an actual minority-majority term. By padding with dummy variables, any local minority term of an algebra $\mathbf{A}_n$ is also a term that locally satisfies the minority-majority term equations. But since each $\mathbf{A}_n$ has a Maltsev term but not a minority term, then by Theorem 3 it follows that $\mathbf{A}_n$ cannot have a minority-majority term.

6. Deciding minority in idempotent algebras is in NP

The results from the previous section imply that one cannot base an efficient test for the presence of a minority term in a finite idempotent algebra on checking if it has enough local minority terms. This does not rule out that the problem is in the class P, but to date no other approach to showing this has worked. As an intermediate result, we show, at least, that this decision problem is in NP and so cannot be EXPTIME-complete (unless NP = EXPTIME).

We first show that an instance $\mathbf{A}$ of the decision problem $\mathsf{Minority}^{\mathrm{Id}}$ can be expressed as a particular instance of the subpower membership problem for $\mathbf{A}$.

Definition 13. Given a finite algebra $\mathbf{A}$, the *subpower membership problem* for $\mathbf{A}$, denoted by $\mathsf{SMP}(\mathbf{A})$, is the following decision problem:

- INPUT: $\vec{a}_1, \dots, \vec{a}_k, \vec{b} \in A^n$
- QUESTION: Is $\vec{b}$ in the subalgebra of $\mathbf{A}^n$ generated by $\{\vec{a}_1, \dots, \vec{a}_k\}$?

To build an instance of $\mathsf{SMP}(\mathbf{A})$ expressing that $\mathbf{A}$ has a minority term, let $I = \{(a, b, c) \mid a, b, c \in A \text{ and } |\{a, b, c\}| \leq 2\}$. So $|I| = 3|A|^2 - 2|A|$. For $(a, b, c) \in I$, let $\min(a, b, c)$ be the minority element of this triple. So

$$\min(a, b, b) = \min(b, a, b) = \min(b, b, a) = \min(a, a, a) = a.$$

For $1 \leq i \leq 3$, let $\vec{\pi}_i \in A^I$ be defined by $\vec{\pi}_i(a_1, a_2, a_3) = a_i$ and define $\vec{\mu}_A \in A^I$ by $\vec{\mu}_A(a_1, a_2, a_3) = \min(a_1, a_2, a_3)$, for all $(a_1, a_2, a_3) \in I$. Denote the instance $\vec{\pi}_1$, $\vec{\pi}_2$, $\vec{\pi}_3$, and $\vec{\mu}_A$ of $\mathsf{SMP}(\mathbf{A})$ by $\min(\mathbf{A})$.

Proposition 14. *An algebra $\mathbf{A}$ has a minority term if and only if $\vec{\mu}_A$ is a member of the subpower of $\mathbf{A}^I$ generated by $\{\vec{\pi}_1, \vec{\pi}_2, \vec{\pi}_3\}$, i.e., if and only if $\min(\mathbf{A})$ is a 'yes' instance of $\mathsf{SMP}(\mathbf{A})$ when $\mathbf{A}$ is finite.*

Proof. If $m(x, y, z)$ is a minority term for $\mathbf{A}$, then applying m coordinatewise to the generators $\vec{\pi}_1$, $\vec{\pi}_2$, $\vec{\pi}_3$ will produce the element $\vec{\mu}_A$. Conversely, any term that produces $\vec{\mu}_A$ from these generators will be a minority term for $\mathbf{A}$. □

Examining the definition of $\min(\mathbf{A})$, we see that the parameters from Definition 13 are $k = 3$ and $n = 3|A|^2 - 2|A|$, which is (for algebras with at least one at least unary basic operation) polynomial in $\|\mathbf{A}\|$. For $\mathbf{A}$ idempotent, we can in fact improve n to $3|A|^2 - 3|A|$, since then we do not need to include in I entries of the form (a, a, a).

In general, it is known that for some finite algebras the subpower membership problem can be EXPTIME-complete [10] and that for some others, e.g., for any algebra that has only trivial or constant basic operations, it lies in the class P. In [11], P. Mayr shows that when $\mathbf{A}$ has a Maltsev term, then $\mathsf{SMP}(\mathbf{A})$ is in NP. We claim that a careful reading of Mayr's proof reveals that in fact the following uniform version of the subpower membership

problem, where the algebra $\mathbf{A}$ is considered as part of the input, is also in NP.

Definition 15. Define $\mathsf{SMP}^{\mathrm{Un}}$ to be the following decision problem:

- INPUT: A list of tables of basic operations of an algebra $\mathbf{A}$ that includes a Maltsev operation, and $\vec{a}_1, \ldots, \vec{a}_k, \vec{b} \in A^n$.
- QUESTION: Is $\vec{b}$ in the subalgebra of $\mathbf{A}^n$ generated by $\{\vec{a}_1, \ldots, \vec{a}_k\}$?

We base the main result of this section on the following.

Theorem 16 (see [11])**.** *The decision problem* $\mathsf{SMP}^{\mathrm{Un}}$ *is in the class NP.*

While this theorem is not explicitly stated in [11], it can be seen that the runtime of the verifier that Mayr constructs for the problem $\mathsf{SMP}(\mathbf{A})$, when $\mathbf{A}$ has a Maltsev term, has polynomial dependence on the size of $\mathbf{A}$ in addition to the size of the input to $\mathsf{SMP}(\mathbf{A})$. We stress that Mayr's verifier requires that the table for a Maltsev term of $\mathbf{A}$ is given as part of the description of $\mathbf{A}$.

Theorem 17. *The decision problem* $\mathsf{Minority}^{\mathrm{Id}}$ *is in the class NP.*

Proof. To prove this theorem, we provide a polynomial reduction f of $\mathsf{Minority}^{\mathrm{Id}}$ to $\mathsf{SMP}^{\mathrm{Un}}$. By Theorem 16, this will suffice. Let $\mathbf{A}$ be an instance of $\mathsf{Minority}^{\mathrm{Id}}$, i.e., a finite idempotent algebra that has at least one operation.

We first check, using the polynomial-time algorithm from Corollary 7, to see if $\mathbf{A}$ has a Maltsev term. If it does not, then $\mathbf{A}$ will not have a minority term, and in this case we set $f(\mathbf{A})$ to be some fixed 'no' instance of $\mathsf{SMP}^{\mathrm{Un}}$. Otherwise, we augment the list of basic operations of $\mathbf{A}$ by adding the Maltsev operation on A that the algorithm produced. Denote the resulting (idempotent) algebra by $\mathbf{A}'$ and note that $\mathbf{A}'$ can be constructed from $\mathbf{A}$ by a polynomial-time algorithm. Also, note that $\mathbf{A}'$ is term equivalent to $\mathbf{A}$ and so the subpower membership problem is the same for both algebras.

If we set $f(\mathbf{A})$ to be the instance of $\mathsf{SMP}^{\mathrm{Un}}$ that consists of the list of tables of basic operations of $\mathbf{A}'$ along with $\min(\mathbf{A})$ then we have, by Proposition 14, that $f(\mathbf{A})$ is a 'yes' instance of $\mathsf{SMP}^{\mathrm{Un}}$ if and only if $\mathbf{A}$ has a minority term. Since the construction of $f(\mathbf{A})$ can be carried out by a procedure whose runtime can be bounded by a polynomial in $\|\mathbf{A}\|$, we have produced a polynomial reduction of $\mathsf{Minority}^{\mathrm{Id}}$ to $\mathsf{SMP}^{\mathrm{Un}}$, as required. □

7. Conclusion

While Theorem 17 establishes that testing for a minority term for finite idempotent algebras is not as hard as it could be, the true complexity of this decision problem is still open. Our proof of this theorem closely ties the complexity of $\mathsf{Minority}^{\mathrm{Id}}$ to the complexity of the subpower membership problem for finite Maltsev algebras and specifically to the problem $\mathsf{SMP}^{\mathrm{Un}}$. Thus any progress on determining the complexity of $\mathsf{SMP}(\mathbf{A})$ for finite Maltsev algebras may have a bearing on the complexity of $\mathsf{Minority}^{\mathrm{Id}}$. There has

certainly been progress on the algorithmic side of SMP; a major recent paper has shown in particular that SMP($\mathbf{A}$) is tractable for $\mathbf{A}$ with cube term operations (of which a Maltsev term operation is a special case) as long as $\mathbf{A}$ generates a residually small variety [2] (the statement from the paper is actually stronger than this, allowing multiple algebras in place of $\mathbf{A}$).

In Section 3 we introduced the notion of a minority-majority term and showed that if testing for such a term for finite idempotent algebras could be done by a polynomial-time algorithm, then $\mathsf{Minority}^{\mathrm{Id}}$ would lie in the complexity class P. This is why we conclude our paper with a question about deciding minority-majority terms.

Open problem. What is the complexity of deciding if a finite idempotent algebra has a minority-majority term?

References

[1] Clifford Bergman. *Universal algebra: Fundamentals and selected topics*, volume 301 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012.

[2] Andrei Bulatov, Peter Mayr, and Ágnes Szendrei. The subpower membership problem for finite algebras with cube terms. *CoRR*, abs/1803.08019, 2018.

[3] Stanley Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981.

[4] Victor Dalmau. Generalized Majority-Minority Operations are Tractable. *Logical Methods in Computer Science*, Volume 2, Issue 4, September 2006.

[5] Ralph Freese and Matthew A. Valeriote. On the complexity of some Maltsev conditions. *Internat. J. Algebra Comput.*, 19(1):41–77, 2009.

[6] O. C. García and W. Taylor. The lattice of interpretability types of varieties. *Mem. Amer. Math. Soc.*, 50(305):v+125, 1984.

[7] Jonah Horowitz. Computational complexity of various Mal'cev conditions. *Internat. J. Algebra Comput.*, 23(6):1521–1531, 2013.

[8] Alexandr Kazda and Matthew Valeriote. Deciding some Maltsev conditions in finite idempotent algebras. Preprint, 2017.

[9] Keith A. Kearnes and Emil W. Kiss. The shape of congruence lattices. *Mem. Amer. Math. Soc.*, 222(1046):viii+169, 2013.

[10] Marcin Kozik. A finite set of functions with an EXPTIME-complete composition problem. *Theoretical Computer Science*, 407(1-3):330–341, 2008.

[11] Peter Mayr. The subpower membership problem for Mal'cev algebras. *International Journal of Algebra and Computation*, 22(07):1250075, 2012.

[12] Miroslav Olšák. The weakest nontrivial idempotent equations. *Bulletin of the London Mathematical Society*, 49(6):1028–1047, 2017.

[13] Matthew Valeriote and Ross Willard. Idempotent n-permutable varieties. *Bull. Lond. Math. Soc.*, 46(4):870–880, 2014.

Charles University, Prague, Czech Republic
E-mail address: alex.kazda@gmail.com

University of Durham, Durham, UK
E-mail address: jakub.oprsal@durham.ac.uk

McMaster University, Hamilton, Ontario, Canada
E-mail address: matt@math.mcmaster.ca

Charles University, Prague, Czech Republic and Lomonosov Moscow State University, Moscow, Russia
E-mail address: zhuk@intsys.msu.ru